Manufacturing Rev. **8**, 15 (2021)
© E. Yalcinkaya et al., Published by EDP Sciences 2021
https://doi.org/10.1051/mfreview/2021013

**Manufacturing Review**
Available online at:
https://mfr.edp-open.org

RESEARCH ARTICLE OPEN ACCESS

# Empowering ISA95 compliant traditional and smart manufacturing systems with the blockchain technology

Erkan Yalcinkaya[*], Antonio Maffei, Hakan Akillioglu, and Mauro Onori

Department of Production Engineering, Royal Institute of Technology, Stockholm, Sweden

Received: 4 April 2021 / Accepted: 29 April 2021

**Abstract.** Technological advancements in the information technology domain such as cloud computing, industrial internet of things (IIoT), machine to machine (M2M) communication, artificial intelligence (AI), etc. have started to profoundly impact and challenge not only the ISA95 compliant traditional (ISA95-CTS) but also the smart manufacturing systems (SMMS). Our literature survey pinpoints that systems scalability, interoperability, information security, and data quality domains are among those where many challenges occur. Blockchain technology (BCT) is a new breed of technology characterized by decentralized verifiability, transparency, data privacy, integrity, high availability, and data protection properties. Although many researchers leveraged BCT to empower various aspects of industrial manufacturing systems, there is no study dedicated to addressing the challenges impacting the manufacturing systems compliant with the ISA95 standard. Thereby, our study aims to fill the identified research gap systematically. This paper thoroughly analyzes the challenges hampering the ISA95-CTS and SMMS and methodically addresses them with corresponding BCT capabilities. Furthermore, this paper also discusses various aspects, including the weaknesses, of BCT convergence to ISA95-CTS and SMMS.

**Keywords:** Blockchain / smart manufacturing / ISA95 / manufacturing industry / cybersecurity

## 1 Introduction

Traditional manufacturing systems built upon the ISA95 standard have recently evolved into more data-centric smart manufacturing systems. These next-generation solutions are attributed to machine-to-machine (M2M) communication, automation, industrial internet of things (IIoT), and artificial intelligence (AI) capabilities. Technological improvements infer new challenges to the existing and future manufacturing systems. Barenji et al. [1] studied contemporary challenges affecting the manufacturing industry and identified systems scalability, interoperability, information security, and data quality domains as the main pain points.

Smart manufacturing systems (SMMS) have become vastly dependent on cloud-based and geographically distributed manufacturing practices with international supply chain mechanisms. A high focus on distributed manufacturing promotes small but specialized micro manufacturing units that can be geographically dispersed and connected through the internet and cloud. However, the evolution from monolith to micro manufacturing units comes with extensive system integration and interoperability challenges. Zeid et al. [2] studied smart manufacturing, industry 4.0, and cloud manufacturing concepts. They concluded that modern manufacturing systems embody various communication protocols causing significant interoperability and integration challenges.

The cybersecurity incidents in the manufacturing industry have been steadily growing in recent years. The interconnected data-driven smart factory concept certainly increases the risk of cyber-attacks. Besides, maintaining a high level of trust among distributed facilities and ensuring data confidentiality, integrity, availability, and traceability have become utterly vital. Tuptuk and Hailes [3] focused on the cybersecurity aspects of SMMS. Their research demonstrated the rising trend in the number of identified security vulnerabilities and reported security incidents impacting the cyber-physical systems and SMMS.

Quality and operational efficiency are two important key performance indicators that are measured continuously in the manufacturing industry. When all production lines are located inside the same facility, controlling and monitoring a vast number of parameters to ensure demanded quality levels and operational efficiency occurs

[*] e-mail: erkany@kth.se

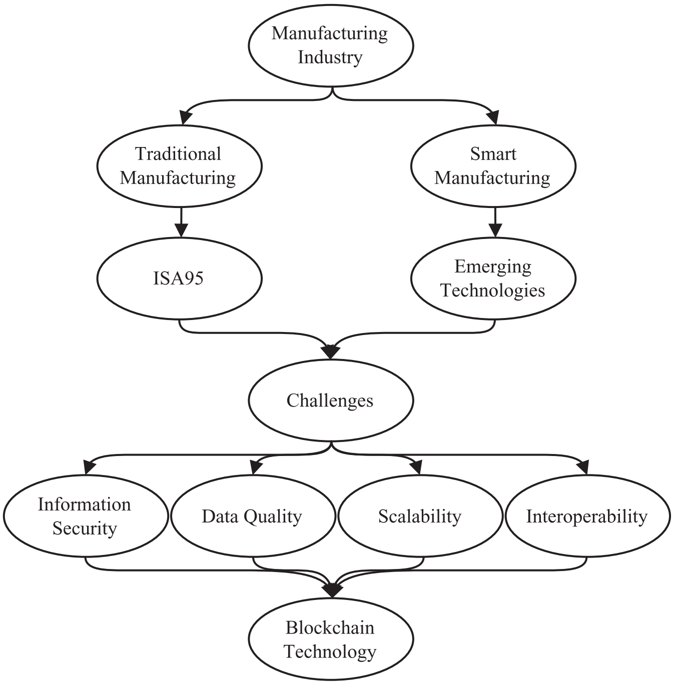

**Fig. 1.** Mind map illustrating the formulation of this research paper.

to be substantially more straightforward than for highly distributed systems functioning beyond the enterprise boundaries. Gifford and Daff [4] researched quality and operational efficiency related to the ISA95 standard and identified significant challenges in these domains.

Blockchain is an emerging technology with distinct characteristics opening new horizons to various business areas, including the manufacturing industry. Blockchain technology (BCT) characteristics are decentralized verifiability, transparency, data privacy, integrity, high availability, and data protection. When individually assessed, none except for decentralized verifiability is exclusive to BCT. In fact, several applications already support some of these characteristics. However, combining all in one platform and providing them as a built-in service for consumption is a capability that makes BCT unique [5,6].

Given the above short introduction, which is illustrated in mind map structure by Figure 1, the purpose of this research paper is to address the following research questions:

- *RQ1:* What are the significant challenges impacting the ISA95 compliant traditional manufacturing systems (ISA95-CTS) and smart manufacturing systems (SMMS)?
- *RQ2:* How can BCT's unique characteristics empower the ISA95-CTS and SMMS to overcome the challenges identified by RQ1?

The rest of the paper is organized as follows: Section 2 summarizes the related work and highlights the research gap. Section 3 clarifies our contribution to the literature, and Section 4 specifies the characteristics of BCT. Section 5 defines the challenges hampering the ISA95-CTS and SMMS and then converges BCT to address them. Section 6 discusses various aspects of BCT convergence to ISA95-CTS and SMMS. Section 7 concludes the research article.

This research article aims to contribute to the scientific literature in different contexts. Firstly, our systematic literature review under Section 5.1 indicates that ISA95-CTS and SMMS suffer difficulties in various fields. We have categorized these areas in systems scalability, interoperability, information security, and data quality domains under the respective subsections. The classification content is enriched with references to relevant research papers and reports available in the literature. Secondly, Section 5.2 converges the BCT to address the categorized challenges. In this context, the BCT's characteristic properties, strengths, and weaknesses are meticulously assessed to address the ISA95-CTS and SMMS challenges. The research content and theoretical discussions are enhanced with several practical examples and their applications as commercial products under the respective subsections. Thirdly, Section 6.1 compares our research with the existing studies conducted to converge BCT with the internet of things (IoT), smart factories, and industry 4.0 applications. Furthermore, in order to maintain the scientific foundation, Section 6.2 discusses the proposed model's weaknesses. Besides, Section 6.3 envisions other research areas that can expand this research with new horizons.Finally, Section 7 summarizes the ISA95-CTS SMMS challenges, corresponding BCT capabilities for remediation, and examples from the literature.

## 2 Related work and research gap

Several researchers have studied BCT and converged blockchain to smart manufacturing, IoT, IIoT, smart factories,and industry 4.0 to address common challenges in respective domains. The following highlights sample research articles selected from the literature as relevant background information related to this research.

Wang et al. [7] compiled a comprehensive review about blockchain for IoT and IIoT. The researchers reported significant challenges with systems interoperability and information security areas profoundly affecting the adoption of IoT and IIoT on a large scale. Moreover, Wang et al. listed BCT's unique properties to overcome the challenges and exemplified several blockchain applications for IoT and IIoT.

Müller and Voigt [8] designed and executed a case study in order to identify the challenges impacting the supply chains in the industry 4.0 context. The case study revealed that insufficient data quality, security, and inconsistent standards are significant challenges against the successful implementation of industry 4.0 capabilities for the supply chain use cases.

Panarello et al. [9] systematically surveyed BCT and IoT integration for seven major application categories, including smart manufacturing. Their research primarily focused on the privacy and security aspects of IoT. Moreover, Panarello et al. [9] justified BCT's convergence to IoT from the confidentiality, authentication, integrity, availability, and non-repudiation standpoints.

Mohamed and Al-Jaroodi [10] analyzed the industry 4.0 applications and challenges impairing the integration of new technologies to the manufacturing value chain. Lack of contract automation, inadequate agreement traceability, and insufficient data security were identified as the major obstacles hampering innovation and agility in the manufacturing industry. Moreover, the researchers specified the design principles (in interoperability, service orientation, decentralization, modularity, real-time capability, and virtualization categories) for the industry 4.0 applications. Furthermore, they elaborated on how BCT can support addressing the reported challenges and fulfilling specified requirements for the manufacturing industry.

Al-Jaroodi and Mohamed [11] executed an extensive survey regarding BCT utilization in various application domains, including but not limited to the manufacturing industry. The researchers highlighted cost reduction, better visibility on value chains, higher energy efficiency, and better machine utilization as the most featured benefits of BCT convergence to the manufacturing industry.

Dai et al. [12] analyzed IoT challenges and identified heterogeneity, complexity, interoperability, resource constraints, privacy, and security as the forefront issues impacting IoT applicability on a large scale. Their research proposition complements IoT with BCT to enhance interoperability, security, autonomy, traceability, and reliability in a broad range of business areas, including smart manufacturing, supply chain management, food industry, smart grid, and healthcare. The research also highlights the benefits of adopting BCT on interoperability when geographical dispersion is the case for intelligent manufacturing. Moreover, Dai et al. [12] stress that BCT explicitly improves system security and addresses privacy challenges in the IoT domain.

Fernandez-Carames and Fraga-Lamas [13] focused on reviewing BCT's application to smart factories defined by industry 4.0. They identified four main benefits of using the BCT, particularly in interoperability and scalability domains. Firstly, multiple systems deployed in a smart factory can vertically integrate through automated M2M communication channels over a ledger. Secondly, BCT can boost the horizontal integration and cooperation of suppliers, manufacturers, and clients through a blockchain-based low latency and extensible communication platform. Thirdly, smart contracts can significantly decrease the reaction time on tasks requiring several manual interactions and automate fast decision mechanisms. Lastly, BCT can promote the inclusion and adaptation of new technologies to industry 4.0 by leveraging the standardized ledger-based data exchange hub.

Fernandez-Carames and Fraga-Lamas [13] also explored the advantages of converging BCT to the IIoT systems and highlighted substantial benefits in enhanced information security and interoperability, improved data access (from the availability standpoint), and standardized communication domains.

Alladi et al. [14] reviewed a wide range of blockchain applications in the industry 4.0 and IIoT context. They performed an extensive survey in several business domains and explored numerous BCT applications. Their key findings can be summarized in four main areas. Firstly, BCT can address security, privacy, data integrity, interoperability challenges and eliminate third-party attestation in the healthcare industry. Secondly, BCT adaptation can be meaningful to address data traceability, integrity, and information security issues in the supply chain industry. Thirdly, the application of BCT is suitable for grid data protection and optimization, as well as seamless integration of heterogeneous entities to the grid ecosystem in the power industry. Lastly, the agriculture industry can leverage BCT to enhance data traceability and reliability.

Alladi et al. [14] also specifically focused on the manufacturing industry. Blockchain is a highly recommended platform to sustain high availability and system robustness to dismiss the threat of malicious attacks. Furthermore, Alladi et al. [14] exclusively favor BCT-based-system solutions to improve system security and data privacy for the IIoT use cases.

As summarized by Table 1, several researchers have studied the challenges related to smart manufacturing, the internet of things (IoT), IIoT, smart factories,and industry 4.0 fields and converged BCT to address common challenges. Thereby, our research intersects with the extant literature from that perspective. However, our literature scanning could not lead to a study dedicated to addressing the challenges impacting the manufacturing systems compliant with the ISA95 standard. Thereby, our research is positioned to fill in the literature gap with novelty in four distinct dimensions. First, the primary focus on ISA95-CTS makes the research context unique. Second, identified challenges are thoroughly analyzed and methodically addressed with corresponding BCT capabilities. Third, the research context concerning information security is enriched with shortcomings reported by the Open Web Application Security Project (OWASP) Top 10 for IIoT report, and the OWASP findings are resolved with specific BCT capabilities. Last but not least, the weaknesses of the proposed model are scientifically discussed.

## 3 Blockchain technology (BCT)

### 3.1 BCT foundation

Although considered cutting-edge technology, the BCT foundation can be described with well-practiced technologies such as cryptographic operations, peer-to-peer protocols, and shared ledger concepts [15].

Singly-linked lists in computer science form a chain-like data formation orderly linking composite data structures with each other. The singly-link list blocks are composed of data and address fields pointing to the previous or next data block in the list. In a nutshell, the blockchain is nothing but a singly-linked list comprised of individual blocks chained with each other by cryptographic hashes of previous block content.

An individual block is composed of two fields in the blockchain. These are header and block content. Although the implementation might differ case by case, the header

**Table 1.** Overview of related references from the literature.

| Paper Ref. | Description |
|---|---|
| Wang et al. [7] | The authors reported significant interoperability and information security challenges impacting the IoT and IIoT. They proposed to converge BCT to overcome the difficulties identified. |
| Müller and Voigt [8] | A case study revealed that insufficient data quality, security, and inconsistent standards are significant challenges against the successful implementation of supply chain use cases for the industry 4.0 capabilities. |
| Panarello et al. [9] | The authors studied IoT and smart manufacturing from the information security perspective and suggested adopting BCT to improve data confidentiality, integrity, availability, ensure source authentication and guarantee non-repudiation. |
| Mohamed and Al-Jaroodi[10] | The authors highlighted lack of contract automation, inadequate agreement traceability, and insufficient data security as the major factors hampering the innovation in the manufacturing value chain and proposed BCT's unique capabilities to address them. |
| Al-Jaroodi and Mohamed [11] | The authors executed a comprehensive survey to determine BCT utilization in a wide range of business areas. They highlighted the BCT benefits in cost reduction, better visibility on value chains, higher energy efficiency, and better machine utilization. |
| Dai et al. [12] | The authors complemented IoT with BCT to enhance data interoperability, information security, system autonomy, data traceability, and infrastructure reliability. |
| Fernandez-Carames and Fraga-Lamas [13] | The authors focused on practical applications of BCT to smart factories and highlighted significant advantages of adopting BCT in data interoperability, systems scalability, and information security domains. |
| Alladi et al. [14] | The authors reviewed a wide range of blockchain applications from the industry 4.0 and IIoT standpoints. The results indicate increased systems availability and enhanced resiliency against malicious activities. |

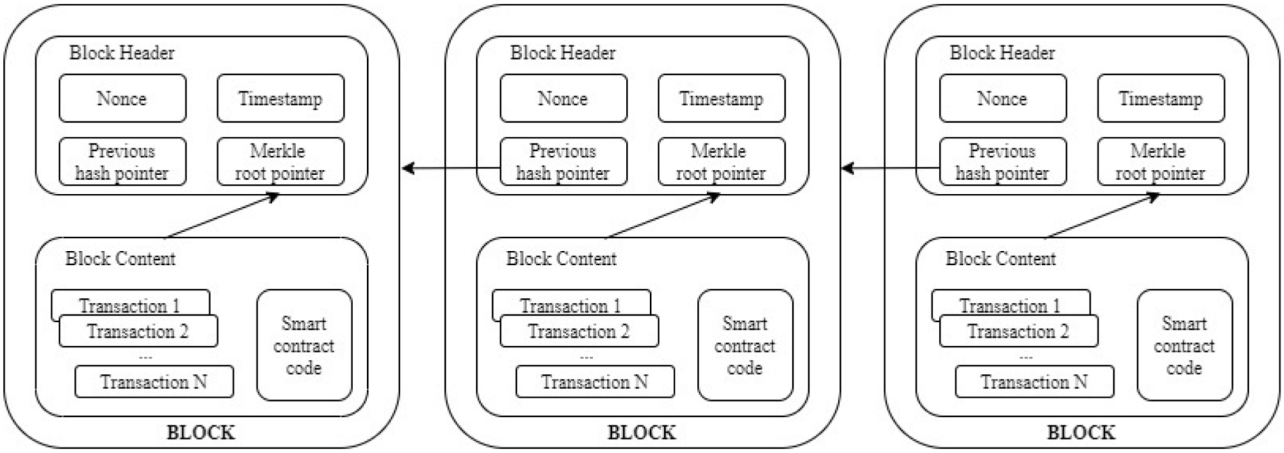

**Fig. 2.** Blockchain structure.

must contain at least the hash value of the previous block as an anchoring pointer, timestamp as the time basis, nonce, and hash of data block (which is also known as the Merkle tree root). Moreover, the block content must contain the collection of confirmed transactions (which are also linked to each other in a tree-like structure, Merkle tree) and smart contract code. Figure 2 illustrates a high-level blockchain structure.

Each transaction in a block content is composed of transactional data and a digital signature. In Bitcoin's case, the transactional data contains the transfer amount and the sender and receiver's identities.

The sender signs each transaction with his/her private key to ensure transactional authenticity, integrity, and non-repudiation of origin. The signed transaction is then broadcasted to the other nodes in the blockchain network via Transport Control Protocol (TCP)-based Point-to-Point (P2P) protocols. Once the transmitted messages are collected, the receiving nodes individually verify every transaction. The heart of the decentralized trust concept boils down to the distributed transaction verification mechanism, eliminating the need for a central authority attesting the transactions.

Dedicated network nodes then collect the verified transactions to produce a new chain block. These dedicated nodes are named miners in Bitcoin terms. Proof-of-work (PoW) and proof-of-stake (PoS) algorithms [16] are among the most popular consensus methods employed by various blockchain platforms. In PoW, the miners first solve mathematically complex puzzles and then compete to link the newly established block to the blockchain to receive an incentive. In PoS, on the other hand, the wealthiest miner (who has the highest amount of coins) has the privilege to link the recently created blocks to the ledger.

In BCT terminology, a ledger is nothing but a database of all linked blocks' full history. From the system architecture point of view, a ledger can be centrally maintained or distributed among all participants or a subset of specially appointed nodes. Although architectural patterns have advantages and disadvantages, distributed architectures have become predominant in recent years due to security, trust, and resiliency concerns [15].

The distributed P2P blockchain can be in three flavors [17].

- *Public blockchains (permissionless)* are fully open to anyone to join or leave without requiring any kind of permission. With this deployment methodology, individual nodes are not trusted, and public consensus to add new blocks to the ledger is needed. The amount of demanded computational power, system resources, and time is substantially higher than the other two alternatives. The highly distributed architecture does not allow rollback, and the transactional throughput is low, whereas the latency is considerably higher. On the other hand, high scalability, high availability, resistance to censorship, and anonymity of transaction holders are the advantages of publicly accessible ledgers.
- *Private blockchains (permissioned)* are exclusively open only for a selected number of participants that are authorized. The system owner grants access and sets the permission levels as well as manages the consensus. The distributed system architecture allows rollback functionality, which is essential for financial applications. Besides, the size of the ecosystem and the number of participants are limited. Because the system is only accessible by selected parties, the computational power demanded by the consensus algorithms is only a fraction of what is required by the public blockchain deployments. Given the low computational footprint and the limited number of participants, systems transactional throughput is much higher, whereas the latency is lower than the other deployment alternatives. Moreover, the closed-loop architecture with individual permissioned access ensures a higher level of security and privacy. Considering the characteristics mentioned above, system architects assess private blockchains as the best match for regulated and complex enterprise applications.
- *Consortium blockchains (permissioned)* can be considered as a unique form of private blockchains. However, with this architectural pattern, multiple participants can form a common inter-organizational (connecting companies, enterprises, etc.) or intra-organizational (connecting different parts of the same organization) operational integration platform. Given the flexibility of supporting a wide range of data exchange patterns, consortium blockchains are the best fit when multiple in-house and partner organizations are involved as the stakeholder.

## 3.2 Characteristics of BCT

The following properties are the main characteristics of BCT [5,6].

- *Decentralized verifiability* can easily be rated as one of the most crucial characteristics of BCT because this feature simply eliminates the need for a central authority to verify individual transactions. For permissionless blockchains, any node can verify a transaction, whereas, for permissioned blockchains, the verification is delegated to assigned peers.
- *Transparency* of a blockchain is ensured through decentralized architecture so that if demanded, multiple independent parties can verify transaction histories.
- *Privacy* has been getting more attention since the General Data Protection Regulation (GDPR) came into force. The amount of personal data being collected and processed by companies has been steadily growing. Therefore, preserving data privacy becomes a big challenge. In the case of permissionless blockchain deployments, a user's identity is anonymized by using unique public addresses. This privacy-preserving technique is ensured by design, and the public addresses are generated by hashing the private key of users. In the case of permissioned blockchains, robust access control mechanisms provide fine-grained control on data privacy. Moreover, data encryption techniques can further improve data privacy for permissioned use cases.
- *Integrity* property ensures that the individual blocks in the blockchain are immutable. In other words, the data is authentic and cannot be deleted or modified by any means. Immutability is guaranteed with individually hashed blocks linked to each other. Therefore, it is impossible to alter any block without disrupting the chain structure. Besides, individually signed transactions guarantee transaction authenticity and integrity.
- *High availability* is a vital system property primarily demanded by business-critical applications. Distributed system architectures are inherently resilient to disruptions; thus, the BCT architecture, regardless of its deployment model, can guarantee high availability and resiliency on the highest possible level.
- *Data protection* is ensured by encrypting data at rest, in transit, and during processing. In all blockchain

**Table 2.** Characteristics of BCT and quality impacts.

| | Permissionless | Permissioned | |
|---|---|---|---|
| | Public blockchain | Consortium blockchain | Private blockchain |
| Decentralized verifiability | **** | *** | ** |
| Transparency | **** | ** | * |
| Privacy | ** | *** | **** |
| Integrity | **** | ** | ** |
| High availability | **** | *** | ** |
| Data protection | ** | *** | **** |

**Table 3.** Benefits and drawbacks of BCT.

| Benefits of BCT | Drawbacks of BCT |
|---|---|
| Immutable, tamper-proof, and timestamped data | Computational resource eagerness *(Concerning permissionless chains)* |
| Decentralized, independent ecosystem and Reduced number of intermediaries and low maintenance cost for end-users | Performance issues *(Concerning permissionless chains)* |
| Transparency and auditability | Privacy concerns *(Concerning permissionless chains)* |
| High scalability and Enabling business automation and excellent data quality | Operational challenges around data immutability |

deployment alternatives, data in transit is protected by encrypted communication channels (Transport Layer Security – TLS). The data protection at rest has twofold. In the first fold, the user utilizes encrypted wallets to store the data at the clientside. In the second fold, depending upon use cases, it is possible to encrypt the block content fully. In this way, data confidentiality increases while transparency decrease. Data protection during processing is an emerging area. There are recently developed cryptographic algorithms, such as homomorphic encryption, that allow operations on encrypted data so that the data is not required to be in a vulnerable unencrypted state, not even during the processing phase.

Table 2 below summarizes the characteristics of BCT and quality impacts [18]. Because there is no established and widely accepted standard describing these properties in practice, it is nontrivial to compare them and calculate the quality impacts accurately.

## 3.3 Benefits and drawbacks of BCT

The following lines highlight the benefits and drawbacks of BCT [19,20], and Table 3 summarizes them in a single table.

### 3.3.1 Benefits of BCT

The BCT promises distinct benefits in a broad spectrum. First and foremost, BCT is closely associated with immutable, tamper-proof, and timestamped data. These properties guarantee data correctness and transactional traceability that enable a wide range of business applications to consume the data served through the ledger as the single source of truth. Furthermore, the decentralized architecture eliminates the need for a central authority. Therefore, controlling or shutting down a blockchain-based system by capturing the central authority is not possible. With BCT, the trust is not centralized but distributed among the entire ecosystem by employing P2P protocols. Besides, not having a central authority means fewer intermediary allocations. Thus, the system maintenance task becomes more manageable, whereas system flexibility and effectiveness substantially increase.

Highly decentralized architecture and highly replicated data ensure that the infrastructure is exceptionally resilient to even catastrophic disruptions such as natural disasters. Moreover, transparency allows complete blockchain ecosystem visibility, enabling the service consumers to audit and observe the transactions. Besides, distributed blockchain system participants are loosely coupled with each other.

BCT also allows a high level of flexibility for scaling up the ecosystem by adding new participants. The loosely coupled architecture also promotes interoperability and the ability to support legacy systems. Besides, smart contracts offer tamper-proof, transparent end-to-end business automation capabilities and ensure operational excellence and quality by eliminating human errors.

### 3.3.2 Drawbacks of BCT

Despite the unique value proposition, ledger-based technologieshave certain drawbacks and limitations. BCT, especially the publicly available ledgers, is notoriously known to be resource-intensive technology. The high resource demand boils down to solving mathematical puzzles employed by the consensus algorithms that incur computational complexities, demanding high processing capacity, expensive hardware, and more power. Kaur and Gandhi [21] estimate that Bitcoin mining consumes 982 MWh/day and calculated that per mined Bitcoin produces 4000 kg carbon footprint, which is a staggering amount of waste when considering a person on average has 5000 kg carbon footprint per year. Moreover, ever-growing ledgers (especially permissionless) need more storage space to host the transactional data. For instance, the ledger size has already reached 163.34 GB for Bitcoin, whereas 667.10 GB for Ethereum [20]. Furthermore, computationally intensive consensus algorithms affect the performance of permissionless ledgers. Hence, even adding one data block becomes a slow operation.

Aside from performance limitations, permissionless ledgers cannot preserve transactional privacy while protecting individual identities with pseudonymization techniques. This is because all transactional data is replicated across the entire blockchain ecosystem. Moreover, in case of a private key compromise, it would be possible to trace back all historical transactions and link them to the victim.

In rare cases, data immutability might become an issue for specific business scenarios where transaction rollback might be demanded when incorrect data is mistakenly committed to the system. The same concern also applies to the cases where smart contracts are not adequately developed. This is because once the contract code is deployed to the blockchain, it is impossible to change or impact the business flow.

### 3.4 Smart contracts

Contracts are nothing but a formal agreement made among business entities. There is always a 3rd party enforcing and assuring the contractual adherence of committing bodies in classical contractual agreements. These 3rd party entities, such that notaries, banks, etc., are appointed by governmental institutions. Thus, indirectly the national state is in charge of enforcing and assuring the contractual agreements.

Smart contracts convert the standard contractual terms into a piece of code and automatically ensure contractual adherence without needing any 3rd party attestation or enforcement. Therefore, the need for an intermediary or central authority is eliminated. In other words, individual untrusted entities can make deals with each other without requiring any 3rd party attestation or involvement.

Smart contracts are deployed to a blockchain, and from the moment of deployment, they start behaving independently and autonomously. In other words, the contractual terms execute automatically when the conditions are digitally met.

A smart contract lifecycle starts when a developer implements the contractual agreements. The smart contract code is then compiled, signed, and deployed to the blockchain, where the contract logic is allocated an address and storage space. The logic is initiated when the smart contract address is invoked. After execution, the contract state is saved to the ledger. Because the smart contract code is stored and executed on the blockchain, it is impossible to manipulate, impact, or temper the contractual execution [22].

In short, smart contracts ensure deterministic self-execution and full automation. Moreover, they eliminate deliberate (a sign of corruption) or unintentional human errors and dependency on 3$^{rd}$ parties.

## 4 ISA95 in the context of smart manufacturing and industrial internet of things (IIoT)

The manufacturing ecosystem is composed of a broad range of production machines and information technology (IT) systems, presenting intricate enterprise architectures. In order to manage the complexity, Purdue University gathered representatives from the production industry and established foundations of cross-domain standardization. This establishment produced a defacto standard, the Purdue model, drafted as a research paper and published by Williams [23]. The International Society of Automation (ISA) [24] then composed a widely recognized standardization, ISA95 standard, based on the Purdue model. The ISA95 standard defines common data structures, processes, methodologies, terminologies, and functions to standardize manufacturing operations. Therefore, the establishment of an end-to-end manufacturing system becomes more manageable and affordable. In addition, implementation risks such as the risk for failure are substantially mitigated [25].

The ISA95 standard defines a functional hierarchical model to categorize a wide range of enterprise manufacturing functions. This model comprises five layers, known as the automation pyramid [25] (Fig. 3).

- *Level 0* represents the lowest entity in the ISA95 model, where the manufacturing processes are actually realized. At this level, the operational timeframe is in milliseconds [26]. Typically, sensors (pressure, temperature, etc.) and all field devices (actuators, servo motors, etc.) are located at level 0.
- *Level 1* represents the first logic layer, where the data received from level 0 sensors are processed. The manufacturing processes operating on this level rely on constant feedback mechanisms. Programmable logic controller (PLC) interfaces are located in level 1, and the operational timeframe is in seconds.
- *Level 2* represents the automation layer where the process operation, automation, and controls take place. Human Machine Interfaces (HMI), Supervisory Control and Data Acquisition (SCADA) systems talk to the lower-level protocols such as HMI and PLC via particular communication protocols such as Modbus. Level 2 usualy operates in a minute timeframe.

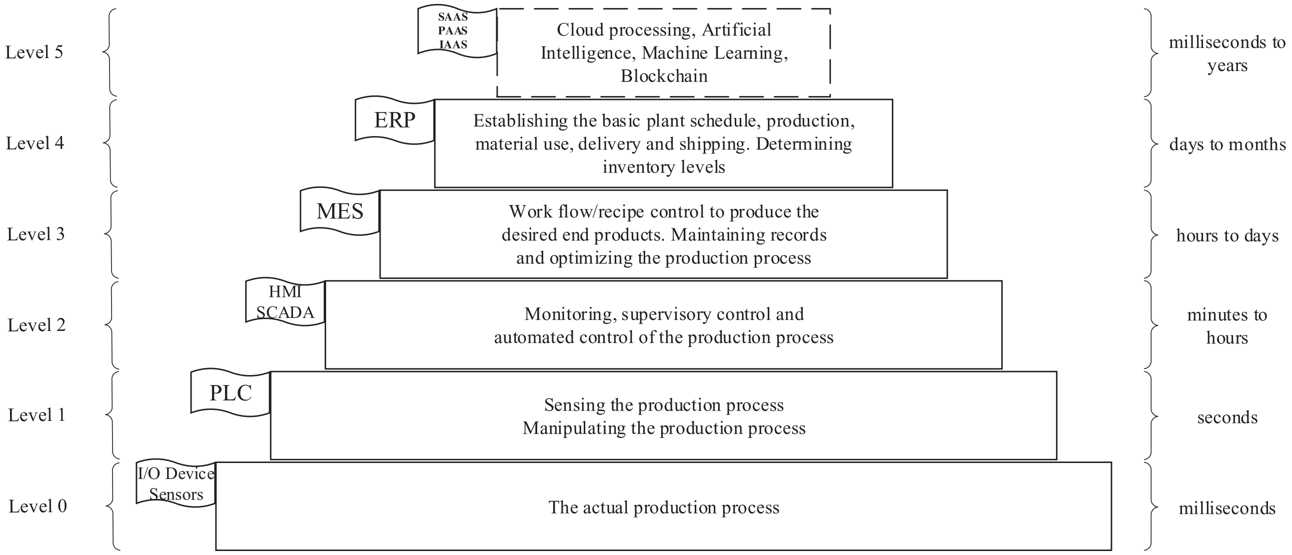
Level 5
SAAS
PAAS
IAAS
Cloud processing, Artificial Intelligence, Machine Learning, Blockchain
milliseconds to years
Level 4
ERP
Establishing the basic plant schedule, production, material use, delivery and shipping. Determining inventory levels
days to months
Level 3
MES
Work flow/recipe control to produce the desired end products. Maintaining records and optimizing the production process
hours to days
Level 2
HMI
SCADA
Monitoring, supervisory control and automated control of the production process
minutes to hours
Level 1
PLC
Sensing the production process
Manipulating the production process
seconds
Level 0
I/O Device
Sensors
The actual production process
milliseconds

**Fig. 3.** Automation pyramid.

- *Level 3* represents the workflow layer on which the product specifications and detailed production cookbooks are defined and maintained. Moreover, level 2 operations are coordinated and supervised. Manufacturing Execution Systems (MES) typically operate at this level, and MES rarely talks to the lower layers. In the classical ISA95 architectures, human operators read data from level 2 and input it to MES. Due to the involvement of human intervention, the operational timeframe spans commonly from hours to days.
- *Level 4* represents the enterprise resource planning (ERP) and logistics layer, where the business planning, production scheduling, raw material logistics, and shipping-related functional tasks are performed. Level 4 ERP functions demand significant human intervention and processing. Thus, the operational timeframe span from days to months.
- *Level 5* is not a layer formally defined by the ISA95 standard. However, since the introduction of smart manufacturing and industry 4.0 concepts, the manufacturing industry has started to benefit from technological advancements in IT such as cloud computing (in various forms such as infrastructure as a service (IAAS), software as a service (SAAS) and platform as a service (PAAS)), big data, AI, machine learning (ML) and BCT. Thus, the classical automation pyramid can be extended with a new abstraction layer to accommodate the next-generation technologies. The timeframe in level 5 vastly varies from milliseconds to years, depending upon the use case and technology.

Over the last decade, with the introduction of the smart manufacturing concept, the significance of distributed data has considerably increased. A significant amount of information is collected from various manufacturing processes scattered within the organization and across the vendors. This data is also fed to AI to train ML algorithms, which are then used to develop predictive and proactive intelligent manufacturing models.

IIoT is a new breed of technology that has become popular, especially among those researching in the smart manufacturing domain. With the recent technological advancements, factory shop-level tools (sensors, actuators, etc.) have become extremely accurate, sensitive, and intelligent. Therefore, the operational visibility on manufacturing processes has advanced to a new level for which instant feedback mechanisms and a vast amount of collected data allow AI-based statistical predictive algorithms to enable the manufacturing processes to be more efficient and productive [27].

Ubiquitously distributed computation and telecommunication capabilities transformed the traditional monolith factories (where the end-to-end production process is finalized within the same factory) into distributed micro manufacturing entities that are interdependent on each other to fulfill the interconnected manufacturing processes. IIoT, in this case, contributes to the distributed manufacturing concept by providing deep operational insight and M2M communication capabilities. Consequently, IIoT technology becomes vital to autonomously react to operational changes with fast feedback mechanisms to ensure service quality.

Although the ISA95 standard and the automation pyramid are still applicable to support the smart manufacturing and IIoT technologies, extending the framework with new technical capabilities is deemed necessary [4].

## 4.1 Challenges with ISA95-CTS and SMMS

This section elaborates on challenges affecting the ISA95-CTS and SMMS in systems scalability, interoperability, information security, and data quality domains.

### 4.1.1 System scalability and interoperability challenges

The concept of scalability in industrial and smart manufacturing domains can be studied in IT and non-IT contexts. This research paper only focuses on the IT aspects of manufacturing; therefore, the non-IT perspective is disregarded.

Highly scalable IT systems can seamlessly grow up and down to maintain consistent system throughput regardless of the system load [28].

ISA95-CTS and SMMS commonly rely upon cyber-physical systems, which are, in a sense, small computational units, in other words, computers. Some researchers classify these computational units as multi-agent platforms, whereas others IIoT. Regardless of how they are named, modern manufacturing networks are demanded to host an increasing number of these computational units. Consequently, aging, nonflexible, and predominantly centralized manufacturing system architectures cause scalability bottlenecks [1].

The cost of machines used by modern manufacturing systems is exceptionally high. Moreover, these machines are heavy and customized to perform specialized tasks. Therefore, once they are installed, shop-level machines serve for a long period, and it would be challenging to replace them with a newer model. Given this fact, even modern manufacturing lines are composed of a combination of legacy and modern devices. This over-complex diverse ecosystem leads to severe interoperability challenges.

Standardization is one way to manage the complexity of interoperability among legacy and modern devices. Watson et al. [29] listed several industry 4.0 standards, such as IEC 62541, IEC 61850, and IEEE 1722-2016, enabling semantic and syntactic interoperability. However, considering the broad spectrum, even ensuring interoperability among legacy and modern communication standards requires substantial effort. On similar research, Müller et al. [30] investigated the international corporations operating on the industry 4.0 scope from the information-sharing challenges standpoint. Müller et al. [30] reported that noninteroperable and unstandardized interfaces constitute a significant obstacle hampering efficient information sharing in the industry 4.0 ecosystem.

As previously mentioned, the manufacturing pyramid has six levels. The lower levels make use of a broad range of devices and controlling interfaces manufactured by several vendors. The same complexity occurs in the same magnitude in upper layers where the business applications share data and communicate with each other. Pedone and Mezgar [31] studied highly heterogeneous industry 4.0 systems, including modern cyber-physical systems and IIoT, from the cloud adaptability perspective. Their in-depth assessments justify that interoperability and data portability (a form of semantic interoperability) pose the most significant challenge impeding the adoption of new technologies to the complex industry 4.0 ecosystem.

Ray and Jones [32] published a research article elaborating on the integration and interoperability challenges impacting the ISA95 automation pyramid actors. Likewise, Gifford and Daff [4] identified many painpoints in integrating modern plant systems with the existing 150+ system platforms.

### 4.1.2 Information security challenges

According to NTT (international cybersecurity consultancy firm) Global Threat Intelligence Report [33], the manufacturing industry was in the top 3 most attacked industries worldwide in 2019. Compared to the previous year, the amount of malicious activity in 2019 remained consistent. The report associates the malicious activities with the vulnerabilities introduced due to manufacturing ecosystem complexity and extensively interconnected system architectures that rely on IoT and IIoT technologies. The same report also highlights that several manufacturing systems cannot preserve data confidentiality, integrity, availability and cannot ensure data traceability aspects. Consequently, manufacturing systems become more vulnerable to malicious attacks.

Sun et al. [34] focused on smart manufacturing and smart factories from the human wearable sensors standpoint. They identified interoperability, information security, and privacy imperfections with the wearable sensors hamper value creation in the industry 4.0 ecosystem.

Zhang et al. [35] suggest adopting operational data analytics, ML, and AI in the manufacturing field to tackle operational stability challenges. However, the manufacturing companies are reluctant to transform their business to utilize advanced analytical capabilities because of the information security risks related to storing and processing a vast amount of operational data. Likewise, according to Buranello from Telit (IoT manufacturer) [36], modern manufacturing practices aim to extend and diversify production capabilities by making use of IIoT based solutions. However, the adaptation speed is not at the desired level, as 49.2% of the manufacturing companies are reluctant to invest in IIoT due to the security and privacy risks.

Ransomware is malicious software that encrypts critical data or particularly business documents. This type of attack profoundly impacts data availability, as the information becomes inaccessible when needed for legitimate purposes. Various manufacturing and production facilities have been victims of ransomware attacks in recent years [37]. According to BlackFog, a cybersecurity consultancycorporation, the manufacturing business and public sector have been the most targeted industries hit by the ransomware attacks in the first and second quarter of 2020 [38].

Distributed Denial of Service (DDoS) attack is a type of malicious activity impacting the availability of internet-facing systems [37]. DDoS has become more prevalent with Industry 4.0 and smart manufacturing harnessing IIoT and cloud computing infrastructures.

Traditional ISA95 layer 0 to 4 communication protocols (i.e., SCADA, Modbus, etc.) were not designed to be secure and do not even support basic cryptographic functions such as encryption and hashing. Therefore, the majority of the ISA95 communication protocols are vulnerable to a wide range of attack vectors. Chhetri et al. [37] demonstrated an integrity tampering attack that targets Computer-Aided Design (CAD) tools. The proof of work attack alters the 3D printer firmware and design files to produce tampered end

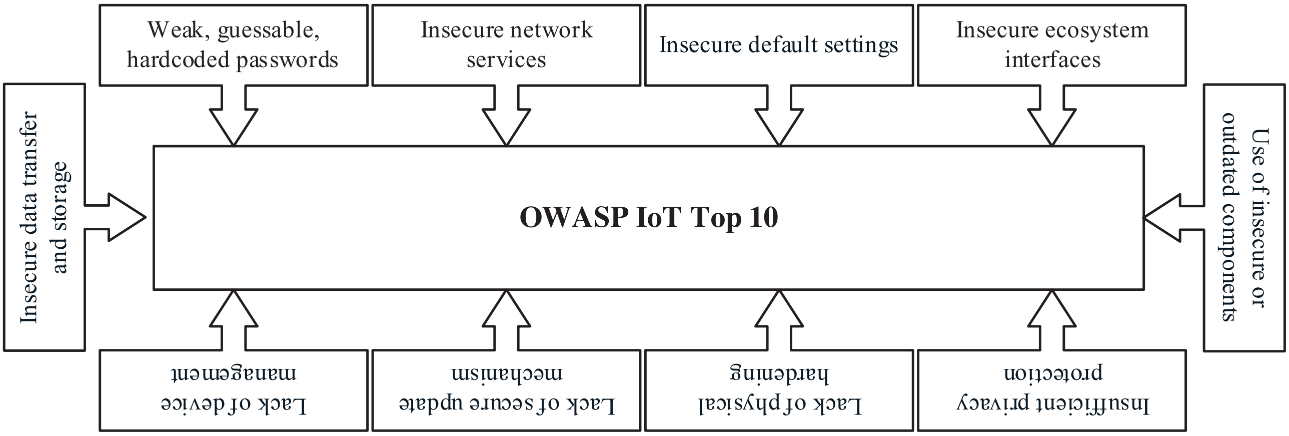
Weak, guessable, hardcoded passwords
Insecure network services
Insecure default settings
Insecure ecosystem interfaces
Insecure data transfer and storage
OWASP IoT Top 10
Use of insecure or outdated components
Lack of device management
Lack of secure update mechanism
Lack of physical hardening
Insufficient privacy protection

**Fig. 4.** OWASP IoT Top 10.

products that are then propagated through the entire supply chain mechanism.

The OWASP is a well-known independent foundation that aims to improve web application security. OWASP publishes articles, develops useful security tools, and creates cybersecurity governance processes. In 2018, OWASP focused on the IoT field and released OWASP IoT Top 10 cybersecurity risks [39]. The following list summarizes the most prominent cybersecurity issues related to IoT and smart devices.

– Weak, guessable, hardcoded passwords
– Insecure network services
– Insecure ecosystem interfaces
– Lack of secure update mechanism
– Use of insecure or outdated components
– Insufficient privacy protection
– Insecure data transfer and storage
– Lack of device management
– Insecure default settings
– Lack of physical hardening.

OWASP IoT Top 10 (Fig. 4) does not directly address the manufacturing industry, but because the SMMS extensively depends on industrial IoT, the same list of risks can also apply to the IIoT based devices deployed to the ISA95 compliant manufacturing systems.

#### 4.1.3 Data quality challenges

In the context of ISA95, the quality assurance function plays a significant role and ensures high production quality by leveraging real-time data feeds. This is because the production quality is directly related to the quality and accuracy of processed data. Moreover, the smart manufacturing concept is built around intelligent devices that can communicate directly (i.e., M2M). These devices can autonomously make fast decisions with operational data. Thus, the success of operational autonomy is closely correlated with the accuracy and speed of M2M communication.

Gifford and Daff [4] highlighted the data quality and consistency challenges with the ISA95 enterprise manufacturing processes. According to their research, aged communication protocols requiring synchronization with the other party are the primary source of quality and consistency issues with the traditional manufacturing systems. This is because the data messages are regularly delayed on delivery or even lost during transmission. Moreover, event data is delivered to an incorrect recipient or corrupted upon delivery due to synchronization issues.

### 4.2 BCT to address the challenges related to ISA95-CTS and SMMS

This section elaborates on how BCT can address the systems scalability, system interoperability, information security, and data quality challenges impacting the ISA95-CTS and SMMS. Figure 5 illustrates avisual representation of detailedISA95-CTS and SMMS challenges and their relationship with BCT.

#### 4.2.1 Addressing system scalability and interoperability challenges

Scalability can be measured with three key attributes, which are system elasticity (ability to add or remove nodes), latency (time required to respond on a request), and throughput (amount of transactions processed per second – TPS).

Regardless of whether being a permissioned or permissionless blockchain, high elasticity and flexibility are the main characteristics of all BCT-based P2P architectures. However, early BCT platforms, especially permissionless ledgers, had difficulties producing high throughput with low latency. The main reason for poor performance was due to computationally intense consensus algorithms required to verify anonymous transactions. For instance, in Bitcoin architecture, the transaction time may take up to 10 min, and the throughput is about 3–7 TPS. On the other hand, the VISA payment platform can easily process more than 2000 TPS [1].

Fortunately, recent technological and architectural advancements have resolved the BCT scalability challenges. These advancements and trivial consensus algorithms allow BCT to meet the low latency and high

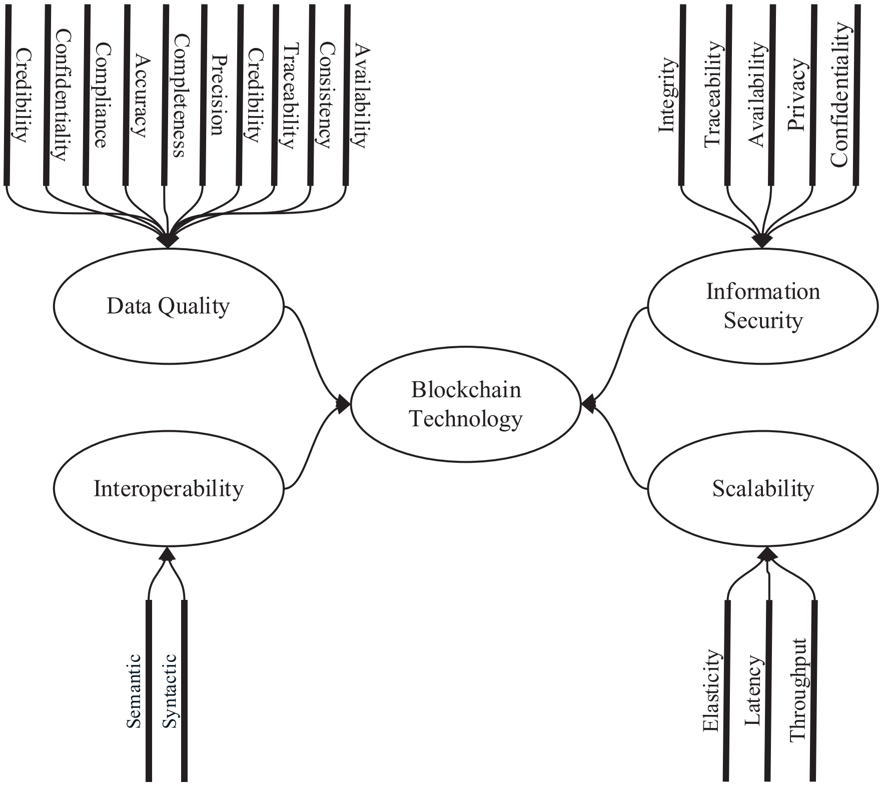

**Fig. 5.** Detailed ISA95-CTS and SMMS challenges and their relationship with BCT.

throughput design requirements. In fact, there are many research articles with proof of concept (POC) implementations available in the literature. For instance, Isaja and Soldatos [40] established a simulation environment with industrial cyber-physical systems and compared two permissioned low latency and high throughput blockchain platforms Neo and Hyperledger Fabric. Their research concluded that the Neo blockchain platform could process up to 1000 TPS, and the Hyperledger Fabric platform can manage up to 1250 TPS.

Brett from SME (non-profit association supportingthe manufacturing industry) [41] reported that Intel collaborated with the IBM Hyperledger community to build an extensive blockchain architecture known as “world wide ledger,” which can process 1500 TPS.

Koens and Poll [42] classified interoperability into two main categories. These can be described in the BCT communication context as follows:

- *Syntactic interoperability* ensures that all communicating parties operate with the same data format and protocol. Syntactic interoperability applies to intra-ledger and inter-ledger data communication use cases. In terms of ISA95-CTS and SMMS, cyber-physical devices produce and consume a vast amount of information that can be converted to a standardized data format and stored on a ledger. Once committed, the information becomes universal data that can be accessed to meet the intra-ledger and inter-ledger data communication use cases. In this way, syntactic interoperability is guaranteed.
- *Semantic interoperability* ensures that all parties talking to each other have a common understanding of data’s meaning. Smart contracts can undoubtedly fulfill the semantic interoperability requirements for the ISA95-CTS and SMMS. Because smart contracts execute autonomously and uniformly in a tamper-proof environment, they can ensure full semantic interoperability.

The smart contract logic is completely detached from the client and fully independent from application logic. They are vendor and supplier agnostic, thus fully supporting cross-platform interoperability. The smart contracts are deployed to a ledger through separate channels, and they have their own application lifecycle. The smart contracts can be developed in various programming languages and provide standardized APIs functioning cross platforms. The access to smart contracts also varies depending upon the business scenario. In other words, smart contracts can be entirely open for anonymous invocations on permissionless blockchain platforms (such as Ethereum [43]). In contrast,they can be restricted to only a subset of authenticated and privileged users on permissioned blockchain platforms (such as IBM Hyperledger Fabric [44]).

Once the syntactic and semantic interoperability requirements are met, a BCT-based manufacturing system becomes a universal data integration platform that can address system dependency and data interoperability challenges. In fact, there are several published articles in the literature proposing to address the legacy dependency and interoperability challenges for the healthcare systems through BCT-based ledgers [42,45]. Randall et al. [45] identified significant interoperability issues and legacy dependences hampering the modernization of healthcare systems. They proposed to overcome the interoperability challenges in two stages. The first stage ensures data standardization through Medicaid Information Technology Architecture (MITA). The standardized data modelsunite the legacy and modern system architectures. Thereby, those systems can syntactically understand each other. The second interoperability layerconstitutes accessing and manipulating data residing on distributed ledgers through unified blockchain Application Programming Interfaces (API). In other words, even if the consumers are different, the interpretation of data is semantically unified.

The blockchain interoperability model elaborated by Randall et al. [45] for the healthcare applications isin line withour proposition to converge the BCT to address the ISA95-CTS and SMMS interoperability challenges. Imposing the ISA95 data model complianceacross the enterprise ecosystem guarantees syntactic interoperability through data standardization. Likewise, smart contracts ensureimpartial blockchain data operations through unified API calls to ensure semantic interoperability.

### 4.2.2 Addressing information security challenges

As highlighted in previous sections, the manufacturing industry experiences significant challenges in preserving data confidentiality, privacy, integrity, as well as ensuring data traceability and availability.

The ISA95 standard concerns primarily the commercial companies for which trade secret protection is essential. Given this prerequisite, we have assumed that employing a publicly accessible (permissionless) blockchain model is not feasible. Hence, the following sections are formulated around this assumption.

#### *4.2.2.1 Data confidentiality and privacy*

As per the above assumption, the permissioned blockchain model forms the first defense line for protecting data confidentiality and privacy.

The data can be in three states in the blockchain. These are data at rest, data in transit, and data during processing (in use). In order to provide full data confidentiality, the BCT should be able to facilitate security mechanisms to protect data in all states.

Communication line security addresses data confidentiality when data is in transit. The BCT communication use-cases are node-to-node (M2M), node-to-ledger, ledger-to-ledger, ledger-to-interplanetary file system (IPFS), and ledger-to-external data sources (Oracles). TLS and Datagram Transport Layer Security (DTLS) protocols are de facto communication and network security protocols that encrypt data while being transported for TCP/IP (internet protocol) and User Datagram Protocol (UDP) packages. Data encryption protects data confidentiality in transit and minimizes the risk of man-in-the-middle attacks.

TLS is equipped with a wide range of cryptographic algorithms, such as forward secrecy, that can preserve the privacy and confidentiality of past data transmissions even if the future encryption keys are compromised.

Khan and Salah [46] investigated the security issues related to IoT devices. Their studies highlighted that authentication and secure communication issues are among the most common security challenges affecting the IoT domain for the TCP/IP and UDP communication protocols. Khan and Salah [46] proposed to mitigate the IoT communication vulnerabilities with a secure blockchain platform protecting the data transmission with TLS and DTLS tunnels.

The data at rest in the blockchain ecosystem can be in various forms, and it is scattered on multiple platforms and systems. Several options and strategies can be employed to protect the data at rest in the BCT ecosystem. Firstly, the data block contents constitute the primary source of blockchain data that is distributed across multiple nodes of the P2P network. In the case of ISA95 enterprise functions related use cases, individual data blocks can contain a wide range of data types, including operational data, transactional data, quality data, order data, etc. Depending upon confidentiality requirements, either the full block content can be encrypted, or a portion of an individual block where the sensitive information exists can be tokenized. Moreover, in the case of highly confidential information that is not allowed to be distributed through the ledger, a special, highly secure file share can protect the data, and file pointers can be circulated through the ledger.

Secondly, blockchain users make use of client-side storage options to store secrets. In Bitcoin terms, the client-side storage component that protects the user's private key is known as "digital wallets." There is no doubt that client-side secrets must be protected with robust encryption algorithms. In fact, the client-side data confidentiality at rest can even be taken to the next assurance level with hardware-based temper proof and encrypted storage options.

Thirdly, a smart contract is nothing but an implementation of business logic, and it can be deployed to the blockchain along with the rest of the data content. A smart contract can be either in stateless or stateful logic. Stateless smart contracts do not demand a storage space, but stateful smart contracts require a nonvolatile space where the execution state, access credentials, private keys, API keys, etc., can be stored. Besides, smart contract execution logic is usually no secret. In fact, in some cases, the source code is fully accessible to ensure business transparency. However, when stateful smart contracts process sensitive information, the state data at rest must be encrypted to ensure confidentiality.

Fourthly, ISA95-CTS and SMMS employ a wide range of cyber-physical systems and IIoT devices, which receive regular system, configuration, and firmware updates. In order to fulfill these operations securely, the confidentiality and integrity of the system maintenance and device administration data need to be assured throughout the entire process. Khemissa et al. (from Cloud Security Alliance) [47] proposed to perform IIoT system maintenance and administrative operations over BCT and focused explicitly on distributing encrypted firmware images and configuration files through blockchain. The proposed method ensures data confidentiality at rest and guarantees a high level of data integrity.

Besides the maintenance use cases, the immutable ledger platforms can also realize IIoT secure asset management and device monitoring use cases.

Fifthly, IPFS is a specialized network storage platform enabling the blockchain P2P network to share and host big data files that are not feasible to distribute over individual data blocks. The files shared over IPFS can be protected on two different levels. Firstly, IPFS filesystem encryption can safeguard the information on the physical hard drive. Secondly, each shared file must be individually encrypted with unique keys.

Lastly, on some occasions, smart contracts require information that does not exist on the blockchain. External data sources (i.e., oracles) are consulted in these cases. The data oracles can fetch data from various data sources such as databases, web services, APIs, and message queues. Because the external sources are highly versatile and mostly outside the blockchain data governance ecosystem, defining security requirements on data confidentiality is not reasonable and outside of this research scope.

The importance of confidentiality during data processing has become vital after the acknowledgment of a new breed of invasive hardware exploits such as row hammer attacks. These attacks aim to access the unprotected process data stored in computer memories where the sensitive data is conventionally unencrypted, thus vulnerable to malicious attacks. In terms of blockchain data and smart contracts, attackers can leak sensitive data in a small window when the data is being processed. Fortunately, recent innovations in cryptography can prevent information leaks when the data is in use. For instance, contrary to traditional encryption algorithms requiring data unencrypted, homomorphic encryption can process encrypted data. Therefore, the information is no longer vulnerable during the processing phase. Benhamouda et al. [48] proposed to combine homomorphic encryption techniques with BCT and demonstrated a POC implementation.

The confidentiality of data is as secure as the strength of the encryption algorithm. Thus, choosing the right encryption algorithm is a delicate task. Because quantum computing has gained significant momentum in recent years, researchers expect that some of the existing encryption algorithms, such as Rivest–Shamir–Adleman (RSA), will be compromised in the coming years. Therefore the BCT proposition empowering the ISA95-CTS and SMMS should employ quantum-resistant encryption algorithms (post-quantum algorithms) to protect the sensitive data [49].

Data privacy is another aspect of data confidentiality, which has become increasingly important since the GDPR came into force. The GDPR mainly concerns protecting personal information, also known as personally identifiable data (PII). Although there are several techniques to assure data privacy, the following are featured, among others.

- The *pseudonymization* technique de-identifies the PII with another unique identifier that is not sensitive. Data encryption, mapping tables, and masking are the most common de-identification methods that are reversible and allow statistical data analysis. Moreover, pseudonymization enables us to reverse the process and reidentify the initial PII value. Reidentification can be possible with the help of reverse mapping tables, data decryption, etc.
- The *anonymization* technique also de-identifies the PII with another unique identifier that is not sensitive. However, the process is entirely irreversible with randomly assigned values, and in most cases, the de-identified data is not useful for statistical data analysis.

Privacy is a significant challenge with distributed ledger and P2P network architectures where the data is inherently scattered on multiple nodes. However, several BCT solutions meet privacy requirements. For instance, IBM Hyperledger Fabric, a permissioned blockchain platform, ensures data privacy with three techniques [50]. Firstly, Hyperledger can establish multiple virtual blockchains on top of the actual physical ledger. The virtual blockchains are formally named channels, and access to the channels can be restricted as required. Secondly, Hyperledger can tokenize PII information with a hash pointer and store the sensitive information in a separate secure database. The hash pointer represents the primary key for the data record and is used to query the actual database. This privacy-preserving method is beneficial, specifically when legal or regulatory requirements entail storing the data in a specific location or region only. Lastly, Hyperledger offers zero-knowledge proof techniques to verify the identities without knowing sensitive information [50].

GDPR assures that individuals could ask to be forgotten when certain conditions are met. In other words, organizations should have technical capabilities and mechanisms to remove personal information from their IT systems upon valid erasure requests. This requirement is fundamentally against the immutability and traceability (full history) characteristics of BCT. However, a few compensating methods are available in the literature to fulfill data removal requirements from the blockchain. One approach is encryption, in which personal data is encrypted. In the case of data erasure requests, wiping the encryption key is sufficient to void the ledger's data [49]. Another advantage of this methodology is that personal data is abolished once for all sub-systems.

Data privacy is and will be a hot topic for legacy and future systems. Although traditional BCT solutions are infamous for preserving privacy, especially concerning permissionless ledgers, BCT can be leveraged to address the IIoT, ISA95, and smart manufacturing privacy challenges with state-of-the-art data management approaches and encryption algorithms.

#### 4.2.2.2 Data integrity, traceability, and availability

An immutable and tamper-proof block structure guarantees data integrity in BCT [49]. Data immutability is ensured by chaining individual blocks to the neighboring blocks with consecutive hashing. Likewise, transaction owners sign transactions with their private keys. Digital

**Table 4.** OWASP IoT Top 10 vs BCT security controls.

| OWASP IoT Top 10 | BCT cybersecurity capability |
|---|---|
| Weak, guessable, hardcoded passwords | N/A |
| Insecure network services and insecure ecosystem interfaces | Built-in and forced communication line security over TLS, authorization with permissioned blockchains, and robust data encryption services |
| Lack of secure update mechanism | Encrypted firmware and configuration file update capability |
| Use of insecure or outdated components | N/A |
| Insufficient privacy protection | Permissioned virtual blockchains structure, data pseudonymization techniques, and zero-knowledge proof techniques |
| Insecure data transfer and storage | Authorization with permissioned blockchains, data encryption at rest, in transit, and use |
| Lack of device management | BCT empowered device management capabilities |
| Insecure default settings | N/A |
| Lack of physical hardening | N/A |

signatures provide non-repudiation and contribute to establishing the tamper-proof platform.

The property of traceability in cybersecurity assures that the full chronological history of all events relevant to any given object exists and accessible when needed. In other words, it is possible to verify who has done what on when. In terms of BCT, every transaction is signed and timestamped when added to the ledger. Because BCT guarantees the chain's state, adding or removing illegal content is impossible. Therefore, all transactional data is transparently traceable and consistently logged since the beginning of the blockchain establishment. In other words, the full chronological history is preserved by design.

The exceptional data integrity and traceability qualities make the BCT-based data preservation and management platforms suitable for a wide range of industries such as healthcare, finance, and manufacturing [42,49].

As highlighted in previous sections, the manufacturing industry has been increasingly the victim of ransomware attacks. There are many techniques to detect and prevent ransomware attacks. Walker from the Fintech Times newsletter [51] proposed a novel approach to harness blockchain's tamper-proof nature to mitigate the ransomware attacks. The integrity of each block is dependent on previous blocks in BCT. Given this property, ransomware cannot encrypt and alter the block content without corrupting the chain structure, which is a significant improvement to prevent ransomware attacks.

DDoS attacks are among the most exploited technique to attack the availability of internet-facing applications for manufacturing organizations. The success of the DDoS attack is closely related to whether the business service is centralized or distributed. In fact, many DDoS prevention techniques rely on distributing the load among several nodes to ensure high availability. There is no single point of failure in terms of BCT infrastructure, which is highly distributed among all nodes. Because there is no central authority (single point of failure) in BCT, performing a successful DDoS attack against all nodes is unlikely. Famous BCT infrastructure, Bitcoin, has managed to endure various cyber-attacks, including DDoS, since it has been operational [49].

Several researchers studied the BCT in the DDoS context. Javaid et al. [52] focused on IoT devices and proposed a BCT-centric DDoS prevention framework. The Ethereumblockchain [43] based POC implementation proved that the BCT could successfully mitigate DDoS attacks using a particular smart contract attribute dubbed "gas." This attribute ensures non-starvation of resources as well as prevents rouge IoT devices from exploiting the BCT network. Shafi and Basit [49] explored BCT capabilities for botnet-based DDoS attacks. The researchers constructed a POC BCT network over a software-defined network (SDN) that enforces network flow rules among different controllers through a ledger. The configurable network rules helpto defeat DDoS attacks by dynamicallyadjusting network rules and containing the malicious nodes.

#### 4.2.2.3 OWASP IoT top10

Given the above-highlighted characteristics and strengths of BCT, we can conclude that the majority of the cybersecurity risk and issues identified by OWASP can be addressed by adopting blockchains for IoT-based use cases [39].

OWASP IoT top 10 concerns ISA95-CTS and SMMS because the manufacturing companies have started to enrich the conventional production systems with smarter cyber-physical devices such as industrial IoT. Table 4 below clarifies how different BCT cybersecurity capabilities can address the common IoT challenges.

### 4.2.3 Addressing data quality challenges

ISO25012 [53] standard defines 15 data characteristics to measure data quality. In our research, we have identified that nine of them apply to the ISA95 standard. The specified data characteristics are essential to benchmark quality requirements. Therefore, at first, the formal definitions of chosen data quality characteristics are provided as follows [53]:

- *Accuracy:* The degree to which data has attributes that correctly represent the true value of the intended attribute of a concept or event in a specific context of use.
- *Completeness:* The degree to which subject data associated with an entity has values for all expected attributes and related entity instances in a specific context of use.
- *Consistency:* The degree to which data has attributes that are free from contradiction and are coherent with other data in a specific context of use. It can be either or both among data regarding one entity and across similar data for comparable entities.
- *Credibility:* The degree to which data has attributes that are regarded as true and believable by users in a specific context of use. Credibility includes the concept of authenticity (the truthfulness of origins, attributions, commitments).
- *Compliance:* The degree to which data has attributes that adhere to standards, conventions or regulations in force and similar rules relating to data quality in a specific context of use.
- *Confidentiality:* The degree to which data has attributes that ensure that it is only accessible and interpretable by authorized users in a specific context of use. Confidentiality is an aspect of information security (together with availability, integrity).
- *Precision:* The degree to which data has attributes that are exact or that provide discrimination in a specific context of use.
- *Traceability:* The degree to which data has attributes that provide an audit trail of access to the data and of any changes made to the data in a specific context of use.
- *Availability:* The degree to which data has attributes that enable it to be retrieved by authorized users and/or applications in a specific context of use.

In terms of data completeness and compliance, the ISA95 standard defines standardized data structures and data templates that can be leveraged across and outside the corporate boundaries. Furthermore, smart contracts in BCT can implement the ISA95 data templates to guarantee the data completeness and compliance properties automatically. Therefore, whenever the data is rendered over the smart contract-based data templates, adherence to the standards is fostered.

BCT has no direct benefit in improving the data accuracy and precision on the shop floor because the ledgers strongly depend on external sources [54]. However, blockchains can preserve and manage data withhigh precision and accuracy. In fact, BCT has been recommended to maintain high data precision in the medical industry [55].

In the previous sections of this research paper, we have elaborated on how BCT can improve data credibility (i.e., non-repudiation and authenticity), confidentiality, traceability, and availability of ISA95-CTS and SMMS. Besides, BCT with robust consensus algorithms and multilayer hashing capabilities always guarantees that the data is in a stable and consistent state. Moreover, the reliability concerns related to aging synchronous communication protocols are resolved with BCT, which practices asynchronous communication.

### 4.3 Overview of converging BCT to address ISA95-CTS and SMMS challenges

Table 5 conveys the high-level overview of the proposed model by listinga point-to-point summary of ISA95-CTS and SMMS challenges, corresponding BCT capabilities for remediation, and examples from the literature.

## 5 Discussions

This section discusses several critical aspects of the proposed modelto converge BCT to address theISA95-CTS and SMMS challenges.

### 5.1 The outlook of BCT in the manufacturing industry

BCT is a disruptive technology and has been a hot topic for many researchers who have been studying in a vast range of application domains. Being a highly researched topic with many unique capabilities, BCT has the potential to shape the future of industry 4.0, smart manufacturing, and cyber-physical systems.

Although offeringunique features and capabilities, the adaptation and acceptance rate for BCTin the manufacturing industry are still not on the desired level. Despite being in 2nd place after financial services for blockchain transformation progress, industrial products and manufacturing industries operating on global markets are still cautiousabout establishinglarge-scale BCT solutions [56]. Regulatory uncertainty and lack of user trust have been identified as the primary barriers against blockchain adoption in respective industries [56].

BCT is a new technology that is still under constant development. New features and capabilities are added continuously to the BCT knowledge base. According to Gartner [57], most BCT capabilities would require 5–10 years of development to reach the plateau of productivity. Gartner also highlights that the majority of the BCT projects couldn't pass the experimental stage. Despite the vast potential, BCT can still notrevolutionize large organizations' digitalization journey [57].

Besides the maturity-related challenges, BCT is also pretty new to the manufacturing industry.Thereby, the enterprise penetration rate and the number of applicable business scenarios are relatively limited. However, with the realization of featured business scenarios, BCT will accelerate the transformation of the conventional manufacturing supply chain and contract management practices to support new business models. Furthermore, BCT has the potential to address the modern and traditional manufacturing industry challenges insystems scalability, interoperability, information security, and data quality areas. By gradually addressing these challenges to ensure smooth cooperation of both legacy and modern systems, BCT will act as a catalyst to accelerate the

**Table 5.** A point to point summary of ISA95-CTS SMMS challenges, corresponding BCT capabilities for remediation, and examples from the literature.

| ISA95-CTS SMMS challenge | BCT capability | Example from literature |
|---|---|---|
| System scalability | 1. Trivial consensus protocols<br>2. Elastic P2P architecture | Intel's Hyperledger based worldwide ledger can process up to 1500 TPS [41] |
| Interoperability | 1. Syntactic interoperability with universal data through blockchain<br>2. Semantic interoperability with smart contracts | Healthcare system legacy dependency and interoperability challenges can be addressed with BCT [42] |
| Information security | *Data confidentiality* | |
| | Data in transit<br>Transport layer encryption with TLS and DTLS | BCT can protect IoT data transmission channels with TLS and DTLS tunnels [46] |
| | Data at rest<br>*1. Data block content:* Full block encryption, partial data tokenization, and highly secure file share<br>*2. Client-side storage:* Robust encryption algorithms, hardware-based temper proof, and encrypted storage options<br>*3. Smart contract:* Sensitive state data encryption<br>*4. IPFS:* Filesystem encryption and individually encrypted files | Encrypted firmware image and configuration files for IIoT system maintenance and administrative operations can be distributed through blockchain [47] |
| | Data in use<br>Homomorphic encryption techniques | Homomorphic encryption techniques can be applied to BCT [48] |
| | *Privacy* | |
| | 1. Pseudonymization techniques with reversible de-identification<br>2. Anonymization techniques with irreversible de-identification | IBM Hyperledger Fabric with virtual blockchains as channels, PII tokenization, and zero-knowledge proof techniques [50] |
| | *Integrity* | |
| | 1. Tamper-proof block structure<br>2. Chained consecutive hashing<br>3. Transaction signing, ensuring non-repudiation. | BCT based data protection platform to prevent ransomware attacks [51] |
| | *Availability* | |
| | 1. No single point of failure<br>2. Highly distributed infrastructure | Bitcoin infrastructure managed to endure various cyber-attacks, including DDoS [49] |
| | *Traceability* | |
| | 1. Every transaction is signed<br>2. BCT preserves the ledger state and consistency | BCT based data preservation and management platforms in healthcare, finance, smart manufacturing industries [42,49] |
| Data quality | *1. Data completeness and compliance:* Smart contract implementation of ISA95 data templates<br>*2. Precision and accuracy:* High precision and accuracy ensured with BCT<br>*3. Stability and consistency:* Guaranteed with robust consensus algorithms and multilayer hashing capabilities<br>*4. Reliability:* Asynchronous communication protocols eliminate reliability issues with legacy manufacturing systems | 9 out of 15 data quality characteristics defined by the ISO25012 [53] standard are relevant. in the medical industry, BCT is a recommended technology for the medical industry requiring high precision [55] |

industry 4.0 revaluation. Furthermore, BCT will also play a key role in fulfilling end-to-endprocess automation, which will loweroperational costs, reduce industrial waste, eliminate human errors, and increase efficiency in the manufacturing industry.

Gartner [57] envisions that BCT will be more interoperable and gain additional capabilities such as smart contract portability and cross-chain operability by 2023. Furthermore, blockchain managed services, a cornerstone for technology transformation, will be available for consumption in a few years. With the additional capabilities and services, BCT's enterprise penetration rate to the manufacturing industry will gain momentum. Eventually, once the plateau of productivity is reached, BCT will foster innovation and caterthe foundation for adaptation of new technologies (AI, ML, IIoT, etc.) to the manufacturing industry.

## 5.2 The weaknesses of the proposed model

The weakness of the proposition for ISA95-CTS and SMMS mainly relates to BCT. The limitations can be categorized in the following areas:

- **Information security:** Malicious actors targeting BCT can exploit the following elements.
  - *Private keys:* The secrecy of private keys has always been crucial in ensuring data confidentiality. Thereby, IT applications protect these keys in tamper-proof environments. In BCT terminology, digital wallets represent tamper-proof environments. Song et al. [58] highlighted that vulnerable and improperly managed digital soft-wallets constitute a significant attack vector against blockchain users.TheISA95-CTS and SMMS actors producing and consuming data through a distributed ledger are identified with private keys. The majority of manufacturing devices, including IoT and IIoT, are notorious for low processing power and scarce resources. Given these challenges and infrastructure complexity, insufficiently protected private keys would become a remarkable attack surface to compromise a blockchain-based ISA95-CTS and SMMS.
  - *Blockchain:* Song et al. [58] described three malicious activities that could be classified under this category. Sybil and 51% attacks refer to scenarios where malicious actors produce or acquire multiple nodes intending to impact the blockchain stability and integrity. Eyal and Sirer [59] proved a more comprehensive but less resource-intensive attack, selfish mining, which allows a malicious actor to control a blockchain infrastructure by influencing less than 25% of all nodes. Song et al. [58] also highlighted the importance of network routing for BCT. A malicious actor targeting the blockchain network routing infrastructure would disrupt the internal consistency and integrity. Nodes that are not synchronized accordingly would start throwing time-outs and cause consistency failures across the blockchain ecosystem. The permissioned blockchain deployment models offer the best match for the ISA95-CTS and SMMS ecosystem. Despite increasing the system's security by restricting access to unauthenticated users, permissioned models are more sensitive to Sybil and selfish mining attacks. This is because the number of nodes required to affect the ledger's consistency is substantially fewer than the permissionless equivalents. The same drawback also applies to the network-based blockchain routing attacks, such that influencing the global internet is way more challenging than acquiring a permissioned small-scale network.
  - *Smart contracts:* Praitheeshan et al. [60] surveyed smart contract vulnerabilities affecting the Etherium blockchain platform. Because smart contracts are simply a piece of code running on ledgers, prominent application security issues such as buffer overflow, race condition, improper file access, coding complexity, and bugs make smart contracts vulnerable to a whole range of attacks.Aside from business use cases, this research proposes to harness the smart contracts to address the ISA95-CTS and SMMS semantic interoperability and data quality challenges. In other words, smart contracts play a significant role in empowering ISA95-CTS and SMMS with BCT. Thereby, all present and future vulnerabilities exploiting the smart contract concept will eventually threaten the proposed model.
- **Total cost of ownership:** Adaptation of new technology has always been painful and costly. BCT is no exception to this. Alladi et al. [14] reviewed blockchain applications for Industry 4.0 and IoT in a broad range of business domains. They reported higher costs on enabling IoT for blockchain in the agriculture industry and increased integration costs affecting the supply chain industry. Furthermore, the e-commerce and retail industry's minor companies refrain from adopting BCT because of soaring investment and maintenance costs. Therefore, the proposed BCT-based model would be expected to increase the total cost of ownership for the ISA95-CTS and SMMS ecosystem.
- **Efficiency and resource constraints:** ISA95-CTS and SMMS ecosystem comprises a broad range of systems such as cyber-physical systems and IIoT with low computational and storage capabilities. However, the BCT is notorious for its high computational and storage demands. These challenges obstructing BCT adaptation in the IoT context are also identified by Dai et al. [12].
- **Big data analysis difficulties:** Data science is a trending topic in all business domains and industries. A crucial aspect of data science is the data analysis process, which relates to a massive volume of information. The analysis outcomes are then consumed to deduct business processes improvement models. However, with limited processing power and storage capacity, most of the IIoT devices comprising the ISA95-CTS and SMMS ecosystem are not suitable to support big data analysis. Furthermore, despite mitigating the confidentiality and privacy issues with the modern and legacy manufacturing systems, pseudonymized and encrypted ledger content hampers big data analysis in BCT [12].

## 5.3 Future research areas

This research is constructed around the information collected from the literature. Therefore, the discussion scope mainly concerns the theoretical aspects of ISA95-CTS and SMMS challenges. A follow-up study may explore the practical challenges affecting ISA95-CTS and SMMS with case studies.

Although blockchain is a crucial technology to overcome the predominant issues affecting ISA95-CTS and SMMS, our literature survey could not lead to a system blueprint to guide solution architects to build a blockchain-based solution in the ISA95-CTS and SMMS context. Therefore, a complementary research activity may develop a system reference architecture and describe the system components in depth.

Moreover, another research effort can focus on the proposed model's practical applications and scientifically justify the correctness of converging BCT to ISA95-CTS and SMMS with quantitative results.

This paper characterizes interoperability by technical means from the system-to-system communication standpoint. Thus, business aspects, such as stakeholder interoperability and management, are excluded from the research context. A proceeding article may broaden the research scope by exploring the business aspects of converging BCT to industry 4.0 applications.

## 6 Conclusion

The technological advancements in the manufacturing industry deeply impacted ISA95-CTS and SMMS. This research paper has identified that systems scalability, interoperability, information security, and data quality domains are the most impacted and challenged areas in this respect.

BCT is an emerging technology coming up with several advanced features that can address the manufacturing challenges. Smart contracts enforcing syntactic and semantic operability requirements can be the solution for interoperability challenges. Likewise, high-performing permissioned blockchain solutions with high throughput and low latency features can address the interoperability challenges.

On the information security front, transport layer security can protect the data in transit, and robust quantum-resistant encryption algorithms can ensure high confidentiality when data is at rest. Likewise, homomorphic encryption techniques can be employed to secure the data when in use. Moreover, permissioned virtual blockchains with data pseudonymization and anonymization methods coupled with zero-knowledge identity proving practices preserve data privacy. Besides, a tamper-proof and immutable block structure ensures data integrity. Moreover, the timestamped chronological history of all events provides full data traceability. Furthermore, the distributed blockchain architecture eliminates any single point of failure. Thereby, BCT-based platforms are highly available.

Finally, BCT can provide a sufficient level of assurance to meet the selected ISO25012 data quality requirements, which, in return, address the data quality challenges with ISA95-CTS and SMMS. Table 5 under Sub-Section 5.3 summarizes the proposed model to converge BCT to address theISA95-CTS and SMMS challenges.

## References

1. A. Vatankhah Barenji, Z. Li, W.M. Wang, G.Q. Huang, D.A. Guerra-Zubiaga, Blockchain-based ubiquitous manufacturing: a secure and reliable cyber-physical system, Int. J. Prod. Res. (2020)
2. A. Zeid, S. Sundaram, M. Moghaddam, S. Kamarthi, T. Marion, Interoperability in smart manufacturing: research challenges, Machines **7** (2019) 1–17
3. N. Tuptuk, S. Hailes, Security of smart manufacturing systems, J. Manuf. Syst **47** (2018) 93–106
4. C. Gifford, D. Daff, ISA-95 evolves to support smart manufacturing and IIoT, New challenges and opportunities for manufacturing technologies and standards across industries, ISA, 2018. https://www.isa.org/intech-plus/2018/feb/isa-95-evolves-to-support-smart-manufacturing-and-iiot/ (accessed April 28, 2021)
5. K. Wust, A. Gervais, Do you need a blockchain?, *Proceedings – 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, pp. 45–54, 2018
6. J. Lee, M. Azamfar, J. Singh, A blockchain enabled cyber-physical system architecture for Industry 4.0 manufacturing systems, Manuf. Lett. **20** (2019) 34–39
7. Q. Wang, X. Zhu, Y. Ni, L. Gu, H. Zhu, Blockchain for the IoT and industrial IoT: a review, Internet of Things **10** (2020) 100081
8. J.M. Müller, K.I. Voigt, The impact of Industry 4.0 on supply chains in engineer-to-order industries – an exploratory case study, IFAC-Papers OnLine (2018) 122–127
9. A. Panarello, N. Tapas, G. Merlino, F. Longo, A. Puliafito, Blockchain and iot integration: a systematic survey, Sensors (Switzerland) **18** (2018). doi: 10.3390/s18082575
10. N. Mohamed, J. Al-Jaroodi, Applying blockchain in industry 4.0 applications, In: *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, pp. 852–858, 2019
11. J. Al-Jaroodi, N. Mohamed, Blockchain in industries: a survey, IEEE Access **7** (2019) 36500–36515
12. H.-N. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: a survey, J. Internet Serv. Info. Secur. **9** (2019) 1–30
13. T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the application of blockchain for the next generation of cybersecure Industry 4.0 smart factories, IEEE Acess (2019) 45201–45218
14. T. Alladi, V. Chamola, R.M. Parizi, K.K.R. Choo, Blockchain applications for Industry 4.0 and industrial IoT: a review, IEEE Access **7** (2019) 176935–176951
15. D. Yaga, P. Mell, N. Roby, K. Scarfone, Blockchain technology overview, NIST, 2018
16. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, In: *Proceedings – 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, pp. 557–564, 2017
17. O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, E.B. Hamida, Consortium blockchains: overview, applications and challenges, Int. J. Adv. Telecommun. (2018)
18. X. Xu, I. Weber, M. Staples, X. Xu, I. Weber, M. Staples, *Architecture for Blockchain Applications*. Eveleigh Australia: Springer Nature Switzerland, 2019
19. M. Isaja, A. Calà, Blockchain as a key enabling technology for decentralized cyber-physical production systems, Far-Edge, pp. 1–6 (2020). https://www.edge4industry.eu/wp-content/

uploads/2018/11/Blockchain-as-a-Key-Enabling-Technology-for-Decentralized-CPPS.pdf

20. V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaria, To blockchain or not to blockchain: that is the question, IT Prof. (2018) 62–74
21. G. Kaur, C. Gandhi, Scalability in Blockchain: Challenges and Solutions. San Diego, United States: INC, 2020
22. M. Alharby, A. Van Moorsel, Blockchain-based smart contracts: a systematic mapping study, ArXiv (2017) 125–140. doi: 10.5121/csit.2017.71011
23. T.J. Williams, A reference model for computer integrated manufacturing from the viewpoint of industrial automation, IFAC Proc. **23** (1990) 281–291
24. ISA, International Society of Automation, Automation, International Society of (2021). https://www.isa.org/ (accessed April 28, 2021)
25. American National Standards Institute, ISA-95.00.01-2010, ISA-95.00.02-2010, ISA-95.00.03-2013, ISA-95.00.04-2012, ISA-95.00.05-2013. North Carolina, USA, 2010
26. M. Åkerman, Implementing shop floor IT for Industry 4.0. Department of Industrial and Materials Science, 2018
27. A. Gilchrist, *The Industrial Internet of Things*. Bangken, Nonthaburi, Thailand: Springer, 2016
28. B. Wang, The future of manufacturing: a new perspective, Engineering (2018) 722–728
29. V. Watson, A. Tellabi, J. Sassmannshausen, X. Lou, Interoperability and security challenges of Industrie 4.0, Lecture Notes in Informatics (LNI), Proceedings – Series of the Gesellschaft fur Informatik (GI), vol. 275, pp. 973–985, 2017
30. J.M. Müller, J.W. Veile, K.I. Voigt, Prerequisites and incentives for digital information sharing in Industry 4.0–an international comparison across data types, Comput. Ind. Eng. **148** (2020) 106733
31. G. Pedone, I. Mezgár, Model similarity evidence and interoperability affinity in cloud-ready Industry 4.0 technologies, Comput. Ind. **100** (2018) 278–286
32. S.R. Ray, A.T. Jones, Manufacturing interoperability, J. Intell. Manuf. (2006) 681–688
33. M. Thomas, 2020 Global Threat Intelligence Report (GTIR), NTT, 2020. https://de.nttdata.com/files/2020-en-study-ntt-ltd-global-threat-intelligence-report-2020.pdf (accessed April 25, 2021)
34. S. Sun, X. Zheng, J. Villalba-Díez, J. Ordieres-Meré, Data handling in industry 4.0: interoperability based on distributed ledger technology, Sensors (Switzerland) **20** (2020) 1–22
35. W. Zhang, Y. Shi, S. Duan, J. Liu, Industrial big data analytics, In: *2015 IEEE/ACM 1st International Workshop on Big Data Software Engineering*, pp. 1–3, 2015
36. R. Buranello, The challenges of scaling and securing manufacturing IoT solutions, Telit, 2018. https://www.telit.com/blog/the-challenges-of-scaling-and-securing-manufacturing-iot-solutions/ (accessed April 28, 2021)
37. S.R. Chhetri, S. Faezi, N. Rashid, M.A. Al Faruque, Manufacturing supply chain and product lifecycle security in the era of Industry 4.0, J. Hardw. Syst. Secur. (2018) 51–68
38. Blackfog, The State of Ransomware in 2020, Blackfog Web, 2020. https://www.blackfog.com/the-state-of-ransomware-in-2020/#%0Ahttps://www.blackfog.com/the-state-of-ransomware-in-2020/ (accessed April 28, 2021)
39. OWASP, OWASP top 10 Internet of Things, OWASP, 2018. https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf
40. M. Isaja, J. Soldatos, Distributed ledger technology for decentralization of manufacturing processes, In: *Proceedings – 2018 IEEE Industrial Cyber-Physical Systems, ICPS 2018*, pp. 696–701, 2018
41. B. Brune, At automate show, blockchain described as 'World Wide Ledger', 2020. https://www.sme.org/technologies/articles/2020/april/at-automate-show–blockchain-described–as-world-wide-ledger/ (accessed April 25, 2021)
42. T. Koens, E. Poll, Assessing interoperability solutions for distributed ledgers, Pervasive Mob. Comput. (2019) 1–45
43. Solidity, Ethereum, 2021. https://ethereum.org/en/ (accessed April 28, 2021)
44. I. Blockchain, IBM hyperledger fabric, IBM Corporation, 2021. https://www.ibm.com/se-en/topics/hyperledger (accessed April 28, 2021)
45. D. Randall, P. Goel, R. Abujamra, Blockchain applications and use cases in health information technology, J. Health Med. Info. (2017) 2–18
46. M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. (2018) 395–411
47. S. Khemissa, Using blockchain technology to secure the Internet of Things, Cloud Security Alliance, 2018. https://downloads.cloudsecurityalliance.org/assets/research/blockchain/Using_BlockChain_Technology_to_Secure_the_Internet_of_Things.pdf (accessed April 25, 2021)
48. F. Benhamouda, S. Halevi, T. Halevi, Supporting private data on Hyperledger Fabric with secure multiparty computation, IBM J. Res. Dev. (2019)
49. E. Piscini, D. Dalton, L. Kehoe, Blockchain & cyber security, Deloitte, p. 14, 2018
50. E. Androulaki, S.W. Cocco, C. Ferris, Private and confidential transactions with Hyperledger Fabric, IBM developerWorks, 2018. https://developer.ibm.com/tutorials/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowledge-proof/%0Ahttps://www.ibm.com/developerworks/cloud/library/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowled (accessed April 28, 2021)
51. M. Walker, Blockchain, a barrier against ransomware, 2019. https://thefintechtimes.com/blockchain-barrier-ransomware/ (accessed April 25, 2021)
52. U. Javaid, A.K. Siang, M.N. Aman, B. Sikdar, Mitigating IoT device based DDoS attacks using blockchain, In: *CRYBLOCK 2018 – Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Part of MobiSys 2018*, pp. 71–76, 2018
53. ISO, ISO/IEC 25012, International Organization for Standardization, 2008. https://iso25000.com/index.php/en/iso-25000-standards/iso-25012?limit=5&limitstart=0 (accessed April 25, 2021)
54. H.Y. Paik, X. Xu, H.M.N.D. Bandara, S.U. Lee, S.K. Lo, Analysis of data management in nlockchain-based systems: from architecture to governance, IEEE Access **7** (2019) 186091–186107
55. X. Wang, Q. Hu, Y. Zhang, G. Zhang, W. Juan, C. Xing, A kind of decision model research based on big data and blockchain in eHealth, *Web Information Systems and Applications.*

*WISA 2018. Lecture Notes in Computer Science*, vol. 11242 LNCS, pp. 300–306, 2018, doi: 10.1007/978-3-030-02934-0_28

56. P.G.B. Survey, Blockchain is here. What's your next move?, 2018. https://www.pwc.se/sv/pdf-reports/blockchain/Blockchain-whitepaper-blockchain-means-business_What-is-your-next-move.pdf (accessed January 26, 2021)
57. Gartner, Gartner 2019 hype cycle shows most blockchain technologies are still five to 10 years away from transformational impact, 2019. https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact
58. J.C. Song, M.A. Demir, J.J. Prevost, P. Rad, Blockchain design for trusted decentralized IoT networks, In: *2018 13th System of Systems Engineering Conference, SoSE 2018*, pp. 169–174, 2018
59. I. Eyal, E.G. Sirer, Majority is not enough: bitcoin mining is vulnerable, Department of Computer Science, Cornell University, 2014. https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf
60. P. Praitheeshan, L. Pan, J. Yu, J. Liu, R. Doss, Security analysis methods on ethereum smart contract vulnerabilities: a survey, ArXiv, pp. 1–21, 2019. https://arxiv.org/pdf/1908.08605.pdf

**Cite this article as**: Erkan Yalcinkaya, Antonio Maffei, Hakan Akillioglu, Mauro Onori, Empowering ISA95 compliant traditional and smart manufacturing systems with the blockchain technology, Manufacturing Rev. **8**, 15 (2021)